

abcdefgh

STATE OF WASHINGTON

04-6-914-001

BOARD OF INDUSTRIAL INSURANCE APPEALS

2430 Chandler Ct SW PO Box 42401 • Olympia, WA 98504-2401 • (360) 753-6823 • www.biaa.wa.gov

BOARD OF INDUSTRIAL INSURANCE APPEALS USE OF STATE RESOURCES POLICY

1. PURPOSES

- To communicate to Board of Industrial Insurance Appeals (BIIA) employees their responsibilities for ensuring proper use of state resources in accordance with Chapter 42.52 RCW (Ethics in public service) and WAC 292-110-010 (Use of state resources).
- To establish uniform guidelines for proper use of state resources. This policy applies consistently to all types of state resources, as defined in Section 4 below, unless otherwise noted in Section 6 of this policy.
- To help BIIA employees avoid violations of ethics laws and regulations. This policy has been approved by the State Executive Ethics Board and therefore qualifies for "safe harbor" status pursuant to WAC 292-120-035. This status protects a BIIA employee from Ethics Board sanctions for conduct that violates the Ethics in Public Service Act. The protection applies only where the employee has engaged in conduct permitted by this policy, subsequent to the policy's effective date.

2. SCOPE

This policy applies to all employees of the BIIA and any other person, business, or entity who uses state resources in performing services for the BIIA.

3. GENERAL STATEMENT OF PRINCIPLES

Employees are responsible for proper stewardship of state resources. Employees may not use state resources for their own personal benefit or gain (which may include a use solely for personal convenience or to avoid personal expense), or for the benefit or gain of others. Each individual employee who uses state resources, or the employee who authorizes a use of state resources, is responsible and accountable for appropriate use. Personal use, where permitted, should not interfere with another employee or obligate another employee to make personal use of state resources. In addition, employees should ensure that the use of state resources is most efficient in terms of time and resources.

APPROVED
Executive Ethics Board

Date: 4/9/04

B0404-021

4. DEFINITIONS

"State resources" include, but are not limited to, employees and their time; information technology assets such as computers, workstations, data resources, electronic message systems, software, software licenses, SCAN service, fax machines, telephones, cellular phones and Internet connections or accounts; state contracts; copyrighted material; photocopiers; facilities; vehicles; credit cards; supplies; and the state mail service.

"Electronic message systems" means electronic mail (e-mail) systems that store and transmit communications; voice mail systems that store and transmit voice communications; facsimile and imaging equipment that store and transmit images; and all similar systems.

"Internet" means the connection to and use of interconnected networks in the public and private domains to access the World Wide Web, file transfer protocols and other network resources.

"Computers" means BIIA-owned desktop personal computers, laptop computers, PDAs (personal digital assistants), and BIIA servers and other platforms.

"Monitoring" means overseeing employees' phone (SCAN, 1-800), e-mail and Internet activities. In addition to normal audit trail capabilities, special local area network (LAN) management software allows undetected monitoring of any activity on the LAN.

5. AVOIDING AN IMPROPER USE OF STATE RESOURCES

There are two categories of permissible uses:

- a) **Generally permitted** (a.k.a., the "Green Zone") are uses reasonably related to the conduct of the employee's official state duties. These may include uses that relate to an agency-authorized official state purpose (e.g. Combined Fund Drive activities) or promote organizational effectiveness (organizational effectiveness encompasses activities that enhance or augment the agency's ability to perform its mission).
- b) **Permissible under limited circumstances** (a.k.a., the "Yellow Zone") is the occasional and limited personal use of state resources where the use:
 - results in little or no cost to the state;
 - does not interfere with the performance of official duties;
 - is brief in duration and occasional in frequency;
 - does not distract from the conduct of state business;

APPROVED
Executive Ethics Board

Date: 4/9/04

- does not disrupt other state employees and does not obligate them to make a personal use of state resources;
- does not compromise the security or integrity of state information or software; and
- is not a "prohibited use," as set forth below.

c) **Prohibited uses** (a.k.a., The "Red Zone") are proscribed by the State Constitution, state and federal laws, and/or the Ethics in Public Service Act, and are explicitly prohibited by WAC 292-110-010(6):

- Any use for the purpose of conducting an outside business or private employment;
- Any use for the purpose of supporting, promoting, or soliciting for, an outside organization or group, such as a private business, non-profit organization, or political party, unless provided for by law or authorized by the BIIA;
- Any use for the purpose of assisting an election campaign or the promotion of, or opposition to, a ballot proposal;
- Any use for the purpose of participating or assisting in lobbying the state legislature or a state agency head;
- Any private use of state property removed from BIIA facilities or another official duty station, even if there is no cost to the state; or
- Any use related to conduct that is prohibited by a federal or state law or state agency policy. Such use includes, but is not limited to, the promotion of discrimination on the basis of race, creed, color, gender, sexual preference, religion, age, marital status, national origin, or the presence of any sensory, mental or physical disability; sexual harassment; copyright infringement; or other unlawful activity.

Examples of permissible use (as it conforms to Section 5a and 5b above) (this is not all inclusive):

1. Checking on your family member's medical needs or childcare arrangements.
2. Notifying BIIA employees of approved charitable activities.
3. Notifying BIIA employees of milestone events (retirement, deaths).
4. Administering personal Deferred Compensation account activity.
5. Checking on personal medical insurance information on the Health Care Authority website.

6. Brief and infrequent use of the internet to view web sites related to a personal interest, that is not otherwise prohibited.

Examples of prohibited use (this is not all inclusive):

1. Using the Internet to manage a personal investment portfolio.
2. Accessing or attempting to access an inappropriate or prohibited website (See Section 6-Internet).
3. Sending out an email soliciting contributions or assistance for any outside organization or group.

Further information and examples regarding permissible and prohibited use of state resources may be found at <http://www.wa.gov/ethics/faq.htm>. If an employee is unsure about whether a contemplated use is permissible, the employee should consult their supervisor.

6. ADDITIONAL POLICY APPLICABLE TO SPECIFIC STATE RESOURCES Telephone Service

BIIA-owned telephones are provided to employees for conducting state business. Employees may make occasional but limited use of telephone service for their own benefit provided that the use conforms to the limited personal use standards described in Section 5 above. Personal use of SCAN or the agency toll free numbers is prohibited, even if such use is occasional or limited.

Cellular phones are provided to some BIIA employees who have demonstrated a business-related need. Charges for use of cellular phones are usually higher than conventional, wire-based telephone systems. Employees should not use cellular phones when a less costly alternative is safe, convenient, and readily available, even if the cell phone use might otherwise fall within a "permissible use."

Because cellular transmissions are not secure, employees should refrain from communicating confidential information via cell phone. Cell phones should not be used when operating a motor vehicle.

Computers

All BIIA-owned and or leased computers are provided to BIIA employees for conducting state business. Employees may make occasional but limited use of computers for their own benefit provided that the use conforms to the occasional and limited personal use standard set forth in Section 5, above.

Users must not use or install personally owned software and or hardware on BIIA-owned or leased equipment.

APPROVED
Executive Ethics Board

Date: 4/9/04

Remote access is authorized solely for the purpose of accessing agency or work-related e-mail, calendars, and related files.

Remote access is offered only on BIIA-owned/leased equipment, unless specific authorization is granted by management.

Electronic Message Systems

BIIA electronic message systems (e-mail) are provided to employees as productivity tools for conducting state business. Employees may make occasional but limited use of electronic message systems for their own benefit provided that the use conforms to the limited personal use standards set forth in Section 5, above.

E-mail systems may not be secure. Employees should be aware of potential e-mail security problems before transmitting private or confidential messages.

Employees must safeguard against unauthorized access to e-mail. Employees should log off the system when not in use. Employees should be aware of, and take precautions to avoid, the following types of e-mail security violations:

- "Disclosure" may occur when messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read them; or by user failure to maintain password/security or failure to log off the system or "lock" the PC before leaving it unattended.
- "Message modification" is where a user (authorized or unauthorized) alters a message by modifying its contents or delivery time.
- "Masquerading" is where an authorized user appears to the system as a different user (usually one with higher privileges), thereby gaining access to information or resources, or the ability to send messages under the guise of another user.

Electronic Records Are Not Private

E-mail, facsimile transmissions, and voicemail may create a reproducible electronic record. Electronic records may be subject to disclosure under public disclosure law or as part of an audit.

Review of Electronic Messages

In addition to normal audit trail capabilities, special local area network (LAN) management software allows undetected monitoring of any activity on the LAN, including e-mail and Internet.

Monitoring of e-mail systems may occur:

APPROVED
Executive Ethics Board
Date: 4/9/04

- where the construction, maintenance, repair, or operation of e-mail systems require the random monitoring of transmitted or stored electronic messages;
- where necessary to prevent misuse of the system or investigate suspected unauthorized use;
- where, in order to conduct agency business, BIIA managers require data (including e-mail) controlled by employees under their supervision.

Internet

Access to the Internet is provided to BIIA employees as a research and communication tool for conducting state business. To help ensure Internet use consistent with this policy, the BIIA limits employee Internet access through the use of filtering software. Employees may make occasional use of Internet access for their own benefit provided that the use conforms to the limited personal use standards described above in Section 5.

Employees should be prudent while accessing information on the Internet and should not attempt to access inappropriate Internet sites. If an employee accidentally accesses or attempts to access an inappropriate Internet site, he or she should immediately back out of the site (or discontinue their attempt to access the site). The employee should then notify their supervisor of the mistake.

Internet users are not anonymous. Employees' Internet use will be monitored to ensure compliance with permitted uses, as described in Section 5 above. Such monitoring includes an employee's access, or attempt to access, inappropriate Internet sites. The Internet may not be secure. Employees should consider this before receiving or transmitting information or messages.

Employees may not download software from the Internet without the express permission of the BIIA. Where downloading has been authorized, anti-virus programs must be used to detect and cure infection of the BIIA environment.

Unless authorized by BIIA Managers, employees may not use Internet access to download music, listen to the radio, watch or listen to live events, or engage in other non-business activities, even if the use is brief in duration and infrequent as these types of activities may degrade system performance.

7. PUBLIC DISCLOSURE

The BIIA will not provide third parties with access to stored electronic messages without the consent of the sender or recipient, except in special circumstances. These include:

- the need for access to resolve a technical problem with a system;

- providing disclosure required by public disclosure law; or
- aiding investigations of alleged illegal activity or misuse of the system.

Any electronic message that may mature into a public record must be promptly converted to an appropriate format. Once converted, the record is stored pursuant to standard retention guidelines that are monitored by the Public Information Officer in concurrence with the RCW 40.14.

Questions regarding public disclosure requests related to e-mail should be addressed to your supervisor and the Public Information Officer.

8. SANCTIONS FOR VIOLATION OF THIS POLICY

Violations of this policy may result in loss of access privileges and/or disciplinary action up to and including termination of employment.

State regulations do not permit employees to use state resources for personal purposes and then reimburse the state for the cost incurred. However, if a violation occurs, the employee will be required to reimburse BIIA, but the reimbursement does not cure the violation.

Adopted this _____ day of _____, 2004.

Thomas E. Egan, Chairperson

Calhoun Dickinson, Member

Frank E. Fennerty, Jr., Member

(Supercedes Use of State Resources Policy B0498-21; Software Policy B0396-016 and Electronic Messaging Systems Policy B0993-019)

APPROVED
Executive Ethics Board

Date: 4/9/04